IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	NO. 3:24-CR-00151
v.	)	
	)	JUDGE RICHARDSON
MATTHEW ISAAC KNOOT	)	

RESPONSE OF THE UNITED STATES TO DEFENDANT'S MOTION TO DISMISS CERTAIN COUNTS OF THE INDICTMENT

Comes now the United States of America, by and through the undersigned Assistant United States Attorney, Joshua A. Kurtzman, and United States Department of Justice Trial Attorney Gregory J. Nicosia, Jr., and responds to the defendant's Motion to Dismiss Counts 1, 4, 5 & 6 of the Indictment (hereinafter the "motion" or "motion to dismiss"). (DE # 76.) The defendant's motion should be denied because the indictment: (1) sets forth the elements of the charged offenses; and (2) fairly informs the defendant of the charges against which he must defend. At this stage of the proceeding, no more is required. Accordingly, the United States respectfully submits that the defendant's motion should be denied in its entirety and a hearing on the defendant's motion is unnecessary.

I. FACTUAL AND PROCEDURAL BACKGROUND

On August 7, 2024, a Grand Jury in the Middle District of Tennessee returned a six-count indictment charging the defendant in Count One with Conspiracy to Damage Protected Computers, in violation of Title 18, United States Code, Section 371; Count Two with Conspiracy to Commit Money Laundering, in violation of Title 18, United States Code, Section 1956(h); Count Three with Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349; Count Four with Intentional Damage to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and (c)(4)(A)(i)(I); Count Five with Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028(a)(1) and 2; and Count Six with Conspiracy to Cause the Unlawful Employment

of Aliens, in violation of Title 18, United States Code, Section 371. (DE # 3.) Each count sets forth the statutory language for the relevant offense. (*See id.* at ¶¶ 14a, 25, 27, and 29a.)

As alleged in the indictment, from in or about July 2022 through in or about August 2023, the defendant "acted as a facilitator for one or more overseas [information technology or] IT workers using the persona YANG DI and conspired with them to obtain their employment with U.S. companies, perform work remotely, share in the proceeds generated by the remote IT work, and launder the proceeds of the scheme. This remote IT work was to be performed by individuals physically located within the United States, who were authorized for employment by U.S. companies." (DE # 3 at ¶ 6.) Specifically, each of the defrauded companies believed that it had hired a U.S. citizen named Andrew M., whose identity was stolen and used by Yang Di to fraudulently obtain remote IT work. (*Id.* at ¶¶ 8, 17.) As part of the conspiracy, Yang Di and the defendant agreed that the defendant would receive, set up, and host laptop computers shipped by Yang Di's employers to defendant's residences. (*Id.* ¶ 17c.) The defendant then received and hosted laptop computers issued by U.S. companies and addressed to Andrew M.—not Yang Di—at his Nashville, Tennessee residences – all for the purpose of deceiving the companies into believing that Andrew .M. was located in the United States.[1] (*Id.* at ¶¶ 9, 17d.) Following receipt of the laptops, the defendant—all without authorization—logged on to the laptops, accessed the victim companies' networks, and downloaded and installed remote desktop applications. (*Id.* ¶ 9.) The remote desktop applications enabled Yang Di to work from locations outside the United States, in particular, China, while appearing to the victim companies as Andrew M. working from the defendant's residences. (*Id.*) In exchange, the defendant charged DI monthly fees for his services, including flat rates for each hosted laptop and a percentage of DI's salary for IT work, enriching himself off the scheme. (*Id.*)

The indictment provides further detail through numerous overt acts. For example, it alleges that on or about July 11, July 14, and August 8, 2022, DI obtained employment with Company C, B, and A,

[1] The term "residences" is used here because the defendant resided in two separate apartments during the course of the conspiracy.

respectively, all while using the full name and other means of identification of Andrew M. (DE # 3 at ¶¶ 17a, 17b, and 17f.) On or about August 3 and August 8, 2022, DI provided the defendant with the login credentials—that is, a username and password—for the Company B and Company A laptops, respectively, which the defendant used to login to the companies' laptops and install, without authorization, remote desktop applications. (*Id*. at ¶¶ 17e, 17g, and 17h.) On or about June 22, 2023, the defendant again used login credentials to access a second Company B laptop and again install, without authorization, a remote desktop application—specifically, Splashtop Streamer. (*Id*. at ¶ 17m.) Between on or about July 11, 2022, and on or about August 8, 2023, the defendant and his co-conspirators "caused at least $544,700 in damages to Company A, Company B, and Company C, representing the cost to remediate the victim companies' corporate computer networks and devices, audit code created by DI, and pay associated legal fees." (*Id*. at ¶ 17o.) The remediation costs described in the indictment were all the direct results of the charged conspiracy, of which the defendant played an integral role, and were incurred as a result of the breaches to the integrity of the victim companies' networks by the defendant and his co-conspirators.

On October 4, 2024, the defendant filed an unopposed motion to continue trial, which was granted on November 7, 2024. (DE # 16 and 29.) On February 17, 2025, the defendant filed a second unopposed motion to continue trial, which was granted on February 18, 2025. (DE # 39 and 41.) On April 1, 2025, the defendant filed a motion to suppress. (DE # 48.) On April 14, 2025, the government filed its response to the motion to suppress, and on April 28, 2025, the defendant filed a reply to the government's response. (DE # 52 and 55.) On May 6, 2025, the Court ordered supplemental briefing from both parties on three issues related to the defendant's motion to suppress. (DE # 56.) On May 9, 2025, the defendant filed a third motion to continue trial, which was granted on May 22, 2025. (DE # 58 and 70.) Pursuant to that order, trial was rescheduled for August 12, 2025. *Id*. On July 1, 2025, the defendant filed the instant motion to dismiss. (DE # 76).

II. LAW AND ARGUMENT

The Federal Rules of Criminal Procedures provide that a defendant may raise, through a pretrial motion, "defect[s] in the indictment or information; including […] failure to state an offense." Fed. R. Crim.

P. 12(b)(3)(B)(v). For a court to grant a motion to dismiss an indictment for failure to state an offense, it must find that the conduct alleged in the indictment does not satisfy every element of the charged offense. *United States v. Turner*, 615 F. Supp. 3d 576, 579 (W.D. Ky. 2020) (citing Fed. R. Crim. P. 12(b)(3)(B)(v) and *United States v. Maddux*, 917 F.3d 437, 443 (6th Cir. 2019)). Conversely, an indictment is sufficient if it lays out the elements of the charged offense and "'fairly informs a defendant of the charge against which he must defend.'" *Id*. (quoting *Hamling v. United States*, 418 U.S. 87, 117 (1974)). When reviewing the indictment, the court must accept factual allegations as true and "'determine only whether the indictment is valid on its face.'" *Id*. (quoting *United States v. Reed*, 77 F.3d 139, 140 n.1 (6th Cir. 1996); *see also United States v. Hann*, 574 F. Supp. 2d 827, 830 (M.D. Tenn. 2008) (internal quotations omitted)). "When the indictment charges a conspiracy, 'it is well settled that an indictment for conspiring to commit an offense—in which the conspiracy is the gist of the crime—it is not necessary to allege with technical precision all the elements essential to the commission of the offense which is the object of the conspiracy.'" *United States v. Superior Growers Supply, Inc.*, 982 F.2d 173, 176 (6th Cir. 1992) (quoting *United States v. Reynolds*, 762 F.2d 489, 494 (6th Cir.1985)). In sum, a motion under Rule 12(b)(3)(B)(v) must *only* raise questions of law, not fact. *United States v. Ali*, 557 F.3d 715, 719 (6th Cir. 2009)).

The defendant's motion offers a series of misplaced factual arguments to resolve a question of law. The factual allegations of the indictment, which must be accepted as true for purposes of this motion, lay out the elements of each charged offense and inform the defendant of the charges against which he must defend. The defendant's motion, therefore, should be denied.

a. <u>Counts One and Four: Intentional Damage to a Protected Computer</u>

As noted above, the indictment charges defendant with intentional damage to a protected computer in Count One as part of a conspiracy, in violation of 18 U.S.C. § 371, and in Count Four as a standalone offense, in violation of 18 U.S.C. § 1030(a)(5)(A). The thrust of defendant's motion with respect to the computer fraud allegations is that the indictment fails to allege that the defendant *damaged* a protected computer. (DE # 76 at 5-6.) However, the defendant incorrectly frames the analysis in terms of unauthorized access, rather than damage, to a protected computer. (*See* DE # 76 at 6-7.)

To charge intentional damage to a protected computer, the indictment must allege: (1) the defendant knowingly caused the unauthorized transmission of a program to a protected computer; (2) the defendant caused the transmission of the program with the intent to damage or deny services to a computer or computer system; (3) the defendant thereby caused damage; and (4) the defendant's actions caused a loss aggregating at least $5,000 in value during any one-year period affecting one or more other protected computers. 18 U.S.C. § 1030(a)(5)(A); 2 Modern Federal Jury Instructions-Criminal P § 40A.06 (2023).[2] Here, the elements of the offenses are plainly set forth within the indictment. (*See* DE # 3 at ¶¶ 14-14a and 25.)

With respect to the first element, the indictment alleges that the defendant used login credentials provided to him by DI—that were intended for use solely by Andrew M.—to login to, download, and install, without authorization, remote desktop applications on at least three victim company computers. (*See* DE # 3 at ¶¶ 17e, 17h, and 17k.). A "protected computer" is any computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2). *See Van Buren v. United States*, 593 U.S. 374, 378 (2021) (definition of protected computer under 18 U.S.C. § 1030(e)(2)(B) includes "at a minimum . . . all computers that connect to the Internet"). Here, all of the victim company laptops qualify as protected computers as each laptop was mailed to the defendant's residences to be used to perform work and was connected to and accessed from the Internet.

Regarding whether the transmission was "unauthorized," section 1030(a)(5)(A) is the only independent "damage" provision within 18 U.S.C. §1030, meaning it does *not* also require a lack of authorization to access the computer. *Contrast* 18 U.S.C. § 1030(a)(5)(B), (C) (both applying to damage that results from unauthorized access of a computer). Section (a)(5)(A) prohibits "intentionally caus[ing] damage without authorization." Numerous courts have recognized in discussing both the damage and access provisions, the ordinary meaning of "without authorization" is "without permission." *See United States v.*

[2] The current Sixth Circuit Pattern Jury Instructions do not contain instructions for any of the computer fraud offenses set forth at 18 U.S.C. § 1030.

Thomas, 877 F.3d 591, 595 (5th Cir. 2017); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (quoting Random House Unabridged Dictionary to define "authorization" as "permission or power granted by an authority"); *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015) (same); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (defining "without authorization" as "without approval"); *United States v. Yucel*, 97 F.Supp.3d 413, 422 (S.D.N.Y. 2015) (citing Webster's Third International Dictionary). Thus, a defendant's transmission of code that caused damage must have occurred without permission, but this provision of the statute does not also require a lack of authorization to access the computer (even if such unauthorized access arguably occurred). *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 301 (6th Cir. 2011).

With respect to the second and third elements, the term "damage means" "*any* impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (emphasis added). By downloading and installing remote access software without permission, the defendant impaired the integrity of data and information on these systems and the systems themselves. By its very nature, remote access software creates a connection between two computers (via the remote desktop protocol) that allows the computer to be controlled remotely. Where a company's device was not authorized by its owner—here, Companies A, B, C, and D—to make such a connection, that is an impairment of the system because it circumvents the security controls put in place by the owner to protect the device, the company network, and company data. (*See, e.g.*, DE # 3 at ¶ 17l.) Thus, the alteration of the laptop's baseline security controls is itself an impairment, as it is a change to the way in which the computer operates that was unintended. In addition, the unauthorized installation of remote desktop software impaired the integrity of the devices (and the data and information thereon) because it exposed those devices and company networks to the Internet—that is, it created a vulnerable access point that did not previously exist. Finally (and to state the obvious), the defendant's actions impaired the integrity of the devices and the company networks accessible through them by enabling unauthorized individuals, that is DI, to remotely access the device, the corporate network accessible from that device, and the company's data.

In *United States v. Yücel*, Alex Yücel was indicted for developing a remote access tool ("RAT") called Blackshades in violation of, among other things, 18 U.S.C. § 1030(a)(5)(A). 97 F. Supp. 3d 413, 416 (S.D.N.Y. 2015). Yücel moved to dismiss from the indictment the Section 1030(a)(5)(A) charge as void for vagueness, as applied to him, and specifically that the terms "protected computer," "damage," and "without authorization" were unconstitutionally vague. *Id.* at 417. Regarding the term "damage," Yücel argued that "remote access tools are perfectly legal and are used by system administrators to manage and test computer systems everywhere. In many workplaces, for instance, an employee experiencing trouble with his work computer can call a support hotline and allow a computer systems expert to take control of the computer and solve the problem." *Id.* at 421.

The Court rejected Yucel's arguments based on the plain meaning of the statute. *Id.* at 420-21. Finding no controlling appellate opinion construing the definition of "damage," the Court began its analysis by determining the ordinary meaning of the operative terms within the definition: impairment and integrity. *Id.* at 420. It found that integrity means "'[t]he condition of not being marred or violated; unimpaired or uncorrupted condition; original perfect state; soundness'" and that impairment means "'deterioration; injurious lessening or weakening.'" *Id.* (internal citations omitted); *accord Pulte Homes, Inc.*, 648 F.3d at 301. Based on these definitions, the Court concluded the Blackshades RAT, as alleged, caused damage by "'impairing the integrity'" of the victims' computer systems." *Id.* The Court reasoned that "[w]hen taken out of the box, an individual's new computer device operates *only in response to the commands of the owner*. *Id.* (emphasis added). However, "when the Blackshades RAT [was] surreptitiously loaded onto a computer, the computer no longer operate[d] only in response to the commands of the owner." *Id.* Instead, it was now cable of being "*operated by unauthorized users* who have the capability of extracting confidential information from the computer's hard drive. This, if proven at trial, would 'impair' the 'uncorrupted condition' of the computer system, and thus constitute 'damage,' *because the system no longer operate[d] as it did when it first came into the owner's possession and has an unwanted characteristic*, which, if known, would negatively impact the economic value of the computer system, *unless time and money are expended to remove it*." *Id.* (emphasis added). Yücel is analogous to the instant case because

once the defendant installed the remote access software on the victim companies' laptops, he altered the laptops baseline security configuration, thereby causing "damage" to "protected computer[s]" within the meaning of the statute.

Similarly, in *United States v. Shahulhameed*, defendant Ibrahimshah Shahulhameed was convicted of one count of violating 18 U.S.C. § 1030(a)(5)(A). 629 F. App'x 685, 687 (6th Cir. 2015). Shahulhameed worked as a contractor for Toyota. *Id.* A few hours after being fired, Toyota experienced a cyberattack, which was launched from the defendant's corporate user account. *Id.* At trial, a Toyota representative testified that Shahulhameed's password-protected user account logged in remotely to Toyota's corporate network from his corporate-assigned laptop on four occasions after being terminated. *Id.* Logging in remotely to the Toyota corporate network from a Toyota-owned laptop using an assigned username and password was the only way to access Toyota's servers from outside of Toyota's facilities. *Id.* After gaining access, Shahulhameed modified configuration files for several Toyota systems.[3] *Id.* The Court held that because these changes came from Shahulhameed's laptop and his password-protected user account, a reasonable jury could have found that Shahulhameed damaged a protected computer. *Id.* Importantly, Shahulhameed did not transmit any *per se* malicious code; instead, he transmitted commands to the Toyota system that modified legitimate Toyota systems and software in a way that caused damage. The fact that this software has legitimate, commercial uses is not relevant to the analysis of whether damage was caused.

The holdings in these cases accord with the ordinary meaning of phrase "impairment to [] integrity" as used in the statute. The statute does *not* require the unauthorized program to be malicious; all that is required is the *unauthorized transmission* of a program that *causes damage*. Because the term "damage" incorporates "*any* impairment to integrity," the unauthorized download and installation of legitimate software, such as remote desktop software, in fact damages a protected computer.

[3] At trial, a Toyota representative testified that the configuration changes included: (1) disabling load balancing between ToyotaSupplier.com servers; (2) changing letters in domain names, which made it impossible for servers to communicate with each other; and (3) adding unknown password requirements to administrative consoles. *Id*. at 688.

The defendant's motion cites *United States v. Nicolescu* for the proposition that "to 'cause[] damage,' the program must: (1) result in the deletion, corruption, or unavailability of data or information, or (2) cause a computer to run so slowly it no longer functions as intended." (DE # 76 at 6. (quoting *United States v. Nicolescu*, 17 F.4th 706, 715 n.2 (6th Cir. 2021)). The defendant's argument finds no support in *Nicolescu*, however, because as the full footnote recognizes that:

> "18 U.S.C. § 1030(e)(8) defines 'damage' as 'any impairment to the integrity or availability of data, a program, a system, or information[.]' Applying the same statute in the civil context, [the Sixth Circuit] looked to the ordinary meaning of the terms "impairment," "integrity," and "availability" and defined "damage" for purposes of § 1030(a)(5)(A) as "a transmission that weakens a sound computer system—or, similarly, one that diminishes a plaintiff's ability to use data or a system[.]" *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 301 (6th Cir. 2011). Nicolescu's virus, which caused infected computers to 'run very slowly,' would constitute an 'impairment to the integrity … of … [the] system." *See* 18 U.S.C. § 1030(e)(8). In other words, the virus was a 'transmission that … diminishe[d] a [victim's] ability to use … a system.'…"

Thus, the *Nicolescu* Court's analysis of Section 1030's damage provision—to the extent it engaged in one[4]—was the same as that offered by the *Yücel* and *Shahulhameed* Courts discussed above. *Nicolescu* did not read into the statute a limitation on what constitutes damage to a protected computer that are not found in the statute's text, nor definitions of "impairment," "integrity," and "availability."

Finally, with respect to the fourth element, the indictment alleges that the defendant and his co-conspirators "caused at least $544,700 in damages to Company A, Company B, and Company C, representing the cost to remediate the victim companies' corporate computer networks and devices, audit code created by DI, and pay associated legal fees." (DE # 3 at ¶ 17o.) This element, like all the others, is sufficiently alleged in the indictment.

[4] *Nicolescu* is a *post-conviction* challenge to the district court's denial of a motion for acquittal based on insufficiency of the evidence with respect to an indictment charging a conspiracy with three objects, one of which was a violation of 18 U.S.C. § 1030(a)(5)(A). *Nicolescu*, 17 F.4th at 715. Because Nicolescu challenged *only* the sufficiency of the evidence as to the Section 1030(a)(5)(A) object, the Court assumed the evidence on the two unchallenged objects was sufficient and held that Nicolescu's failure to challenge the sufficiency of the evidence on the other two charged objects was fatal to his claim. *Id.*

b. Count Five: Aggravated Identity Theft

The defendant next challenges the allegations relating to Aggravated Identity Theft. (*See generally* DE # 76 at 7-12.) Paragraph 27 of the indictment alleges each element of the offense, an alleged victim, approximate dates of the offense, and means of identification used. Count Five also incorporates by reference the introductory allegations, object, manner and means, and overt acts of the conspiracy set forth in Count One. (DE # 3 at ¶ 26.) The defendant raises two challenges to Count Five: first, pursuant to the Supreme Court's holding in *Dubin*, the crime of aggravated identity theft has not occurred here; and second, that the indictment does not allege sufficient facts to show the defendant helped or encouraged the commission of the offense. We address each argument *in seriatim*.

In *Dubin v. United States*, David Dubin was convicted of healthcare fraud and aggravated identity theft, where the predicate offense was the healthcare fraud, after he overbilled Medicaid for psychological testing performed by the company he helped manage. 599 U.S. 110, 115–16 (2023). Dubin argued on appeal that "using a means of identification in relation to a predicate offense requires 'a genuine nexus to the predicate offense.'" *Id.* at 117. Ultimately, the Court held that under Section 1028A(a)(1), a defendant "uses" another person's means of identification "in relation to" a predicate offense when the use is at the "crux" of what makes the conduct criminal, not an ancillary feature. *Id.* at 114. Specifically, the means of identification "must be used in a manner that is fraudulent or deceptive." *Id.* at 132.

The defendant's argument with respect to *Dubin* appears to be a factual, rather than legal. The United States does not quarrel with the defendant's assertion that the Supreme Court's holding in *Dubin* is controlling—that is, that the charged aggravated identity theft must be at the crux of the charged conspiracy to generate revenue through remote IT work. However, this seems to be a question for the trier of fact, who with appropriate jury instructions and considering all of the evidence, can decide whether the defendant's use of Andrew M.'s means of identification meets the statutory requirements, as interpreted by the Court in *Dubin*. *See United States v. Ali*, 557 F.3d 715, 719 (6th Cir. 2009) (holding that a "motion under Rule 12 is … appropriate when it raises questions of law rather than fact.").

Nevertheless, the indictment sufficiently alleges that the conspirators misuse of Andrew M.'s means of identification was used in a fraudulent or deceptive manner—that is, at the "crux of what makes the underlying offense criminal, rather than merely an ancillary feature." *Dubin*, 599 U.S. at 114. In the Introduction to the indictment, the United States alleges that North Korea has dispatched thousands of highly skilled IT workers to generate revenue by posing as non-North Korean foreign and U.S.-based remote IT workers, who surreptitiously obtain contracts for remote IT work from companies around the world, including in the United States. (DE # 3 at ¶2.) The introductory allegations further state that North Korean IT workers obtain these remote work contracts by, among other means, providing prospective employers with counterfeit, altered, or falsified identity documents that often combine a photo of the North Korean IT worker with the personally identifiable information ("PII") of another person, including U.S. persons. (*Id*. at ¶3.) Then, in Count One, the indictment states the object of the conspiracy was to "generate revenue through a scheme to obtain remote IT work from U.S. companies for overseas IT workers by downloading and installing software without authorization to enable unauthorized remote access and *using stolen U.S. identities, and other means, designed to obscure the true identities and locations of the overseas IT workers*." (*Id*. at ¶15.) (emphasis added). Next, the indictment sets forth the manner and means by which the defendant and his co-conspirators accomplished the objects of the conspiracy. These included purchasing, stealing, or otherwise obtaining "PII and other information belonging to at least one U.S. person (U.S. Victim 1), which was used to gain employment with U.S. companies as part of the remote IT work scheme," and applying "for jobs at the U.S. companies as U.S. Victim 1 and transmitted false information to those companies, DHS, and SSA as part of an employment eligibility check, to include stolen identity information and fake drivers' licenses." (*Id*. at ¶16a and 16c.) Finally, the indictment sets forth several instances in which Andrew M.'s means of identification were used to fraudulently obtain remote IT work. (*See Id*. at ¶17b and 16f.)

Thus, the indictment makes clear that the misuse of Andrew M's means of identification was at the crux of the underlying conspiracy to obtain remote IT work because the conspirators used Andrew M.'s PII to deceive the victim companies into hiring North Korean, rather than American, IT workers. Indeed, the

defendant's co-conspirators would not and—indeed could not—have gotten the very jobs they sought without using Andrew M.'s identity—or that of another U.S. person—because U.S. companies are not permitted to hire North Korean workers, which is noted in the introductory allegations, as well. (*See id*. at ¶1.)

The defendant's motion cites Justice Gorsuch's concurring opinion in *Dubin* at length for the proposition that the majority's "crux" test is unworkable and that Section 1028A(1)(A) is void for vagueness. (*See* DE # 76 at 9-12). However, Justice Gorsuch's concurrence is not controlling law. Moreover, the defendant's motion does not raise a constitutional challenge the statute, and on that point the majority notes:

> "[T]he concurrence believes that it is too difficult to discern when a means of identification is at the crux of the underlying criminality. *Post*, at 1575 – 1576. The concurrence's bewilderment is not, fortunately, the standard for striking down an Act of Congress as unconstitutionally vague. There will be close cases, certainly, but that is commonplace in criminal law. Equally commonplace are requirements that something play a specific role in an offense, whether that role is articulated as a "nexus," [] a "locus," [] or "proximate cause," []. Such requirements are not always simple to apply. Yet resolving hard cases is part of the judicial job description. Hastily resorting to vagueness doctrine, in contrast, would hobble legislatures' ability to draw nuanced lines to address a complex world. Such an approach would also leave victims of actual aggravated identity theft, a serious offense, without the added protection of § 1028A(a)(1)."

Dubin, 599 U.S. at 132 n.10 (internal citations omitted).

The defendant next argues that the indictment does not allege sufficient facts to show the defendant aided and abetted in the commission of the charged aggravated identity theft. (DE # 76 at 12.) To charge aggravated identity theft under an aiding and abetting theory, the indictment must allege: (1) that the crime of aggravated identity theft was committed; (2) that the defendant helped to commit the crime or encouraged someone else to commit the crime; and (3) that the defendant intended to help commit or encourage the crime. Sixth Circuit Pattern Jury Instructions § 4.01 (2023). The defendant asserts that the indictment is devoid of sufficient facts to inform him of the charge against which he must defend. *See Hamling*, 418 U.S. at 117. However, the indictment makes clear that the defendant and individual the defendant knew as "Yang Di" entered in an agreement in which Yang Di would obtain and perform remote IT work using means of identification belonging to Andrew M. (*See* DE # 3 at ¶6-8.) Thus, the defendant was aware at relevant

times, that as Yang Di was obtaining jobs and generating revenue—thereby committing overt acts in furtherance of the predicate felonies— Yang Di was doing so by using "without lawful authority, a means of identification of another person." 18 U.S.C. § 1028A(a)(1).

c. Count Six: Conspiracy to Cause the Unlawful Employment of Aliens

Count Six, which charges a conspiracy to cause the unlawful employment of aliens in violation of 8 U.S.C. §§ 1324a(a)(1)(A) and (f) sets forth the required elements and "fairly informs a defendant of the charge against which he must defend." *Hamling*, 418 U.S. at 117. To charge a such a conspiracy, the indictment must allege that: (1) two or more persons conspired, or agreed, to commit the crime of Unlawful employment of aliens, 8 U.S.C. § 1324a(a)(1)(A) and (f), as charged in the indictment; (2) the defendant knowingly and voluntarily joined the conspiracy; and (3) a member of the conspiracy did one of the overt acts described in the indictment for the purpose of advancing or helping the conspiracy. Sixth Circuit Pattern Jury Instructions § 3.01A (2023). The elements of the underlying offense are similarly three-fold: (1) the defendant hired, recruited, or referred for a fee an individual for employment in the United States; (2) that individual was an alien; and (3) the defendant knew that the individual was not authorized to undertake the employment.

Here again, the defendant's arguments with respect to Count Six appear to be factual, rather than legal in nature. *See United States v. Ali*, 557 F.3d 715, 719 (6th Cir. 2009) (holding that a "motion under Rule 12 is … appropriate when it raises questions of law rather than fact."). the defendant first asserts there are no facts asserting that he "hired, recruited, or referred for a fee" Yang Di for employment. Interwoven with this argument, the defendant's motion further seems to contend he is absolved from criminal culpability because he is not employer. (DE # 76 at 13.) Beginning with the text of the indictment, it alleges that "YANG DI … was a foreign national residing outside, and not authorized to work in, the United States," who "used the stolen identity of a U.S. citizen to apply for and obtain remote IT work at U.S. companies." (DE # 3 at ¶ 7.) The indictment further alleges the manner and means by which the conspirators obtained said remote IT work, and that the defendant "charged DI monthly fees for his services, including flat rates for each hosted laptop and a percentage of DI's salary for IT work, enriching himself off the

scheme." (DE # 3 at ¶9; *see generally* Count One.) Indeed, the defendant's participation in the scheme—that is, allowing Yang Di to obtain remote work using the defendant's physical and Internet Protocol addresses—was essential to the *conspiracy* to cause the employment an unauthorized alien. As discussed above, the entire scheme boils down to a ruse to trick U.S. employers into hiring North Koreans—who cannot legally work in the United States—using a variety of means, including stolen identities and U.S.-based facilitators. At its core, to be successful, the scheme *requires* unauthorized employment of alien.

Lastly, the defendant contends that Section 1324a(a)(1)(A) "was only intended to impose liability on W-2 *employers* who hire unauthorized aliens…" (DE # 76 at ¶ 12.) (emphasis original.) The defendant cites to the statute and *Chamber of Com. of U.S. v. Whiting*, 563 U.S. 582 (2011) in support of this proposition. Problematically, neither the text of Section 1324a, nor *Whiting* offers any support for argument. Section 1324a does not include any language specifically limiting its application to employers. In *Whiting*, petitioners—the U.S. Chamber of Commerce and several other organizations—filed a pre-enforcement challenge to an Arizona law imposing sanctions on employers who knowingly or intentionally employed unauthorized aliens through, among other things, suspending or revoking the businesses' license to operate. *Whiting*, 563 U.S. 582, 587 (2011). Petitioners argued that the Arizona law's license suspension and revocation provisions were both expressly and impliedly preempted by federal immigration law—specifically, 8 U.S.C. 1324a(h)(2), which states that, "[t]he provisions of this section preempt any State or local law imposing civil or criminal sanctions (*other than through licensing and similar laws*) upon those who employ, or recruit or refer for a fee for employment, unauthorized aliens." *Id.*; 8 U.S.C. 1324a(h)(2) (emphasis added). The Court's analysis focused on the interaction between federal immigration law and state laws regulating the employment of unauthorized aliens. *Id.* After an exhaustive analysis of the historical background and specific Arizona law at issue, the Court held the Arizona law was not preempted because "the State's licensing provisions fall squarely within the federal statute's saving clause and … does not otherwise conflict with federal law." *Id*. at 587. With respect to Section 1324a(a)(1)(A), the opinion provides no analysis nor applicable holdings beyond reciting the elements of the offense and the statutory definition of an unauthorized alien. *Id*. at 589. Accordingly, the defendant's motion should be denied.

CONCLUSION

Based on the foregoing, the United States respectfully submits that the Court should deny the defendant's motion to dismiss and do so without an evidentiary hearing.

Respectfully submitted,

ROBERT E. MCGUIRE
Acting United States Attorney

By: *s/ Joshua A. Kurtzman*

JOSHUA A. KURTZMAN
Assistant U. S. Attorney
719 Church Street - Suite 3300
Nashville, Tennessee 37203-3870
Telephone: 615-401-6617

s/ Gregory Jon Nicosia, Jr.
GREGORY JON NICOSIA, JR.
D.C. Bar No. 1033923
Trial Attorney
National Security Division
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 353-4273
Gregory.Nicosia@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that the above document was filed through the ECF system and will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

Date: July 14, 2025

/s/ Gregory Jon Nicosia, Jr.
GREGORY JON NICOSIA, JR.
Trial Attorney
National Security Division